LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors:
James Gillett
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Kent Rice, Audit Manager
Information Systems Audits

CC: Laurence Hubbard, President/CEO
Patti Grosfield, Internal Auditor
Al Parisian, Chief Information Officer

DATE: November 2008

RE: Information Systems Audit follow-up: Policy Holder System, Montana State Fund
08DP-01 (orig. 07DP-14)

INTRODUCTION
We presented our information systems audit of the Policy Holder System at Montana State Fund (MSF) to the Legislative Audit Committee in November 2007. The report contained two recommendations. The recommendations relate to:

- The implementation of controls to ensure coverage levels in PHS is accurate.
- The implementation of review procedures to identify and remove inappropriate access.

We requested and received information from MSF personnel regarding progress toward implementation of our report recommendations. This memorandum summarizes their response and the audit work conducted to verify the response.

BACKGROUND
MSF is a workers' compensation insurance carrier established by Title 39, Chapter 71, MCA. MSF provides worker's compensation insurance for approximately 30,000 Montana employers. MSF is self-funded through revenues obtained from employer premium payments, and is governed by a seven-member board of directors appointed by the Governor.

As the primary workers' compensation carrier in Montana, both employers and employees rely heavily on MSF for their coverage. Montana employers who choose MSF as their workers' compensation carrier are considered policy holders. Policy holders are required to pay an annual premium based on the type of business they operate and the amount of their annual payroll. By paying the premium, policy holders ensure compensation for their employees injured while on the job. During fiscal year 2006, MSF collected approximately $212 million in premium payments from policy holders, and paid $142 million in past and current fiscal year claims.

To assist in the administration of policy holder accounts and premium payments, MSF operates and maintains a computer system called the Policy Holder System (PHS). Since premium payments fund MSF operations, it is critical payments are calculated and processed in an accurate and complete manner.

FOLLOW-UP DISCUSSION
The following sections summarize the report recommendations, and MSF's progress towards implementing the recommendations.

Coverage Levels
In a typical workers' compensation coverage policy only employees are covered, so MSF offers an elective coverage for employers or policy holders who also wish to be covered. Each year new coverage levels are issued which dictate the minimum and maximum a policy holder will pay if they elect to provide themselves with workers' compensation coverage. Coverage levels must be updated in the PHS by July 1. Our audit showed the current year coverage levels associated with the elected coverage had not been updated for the current fiscal year. MSF relied on a manual update of these levels in the PHS, but had no controls to ensure the manual process occurred or worked. As a result, they were unaware the owner levels had not been updated.

Recommendation #1
We recommend the department develop and implement controls to ensure coverage levels in the PHS are current.

Recommendation Status: Implemented

Following our audit, MSF implemented a documented review process to ensure all authorized updates and changes to PHS, including coverage levels, are reviewed by a business analyst to ensure required updates are made to the PHS. Before the change control process can be closed a form has to be completed and signed verifying authorized changes were appropriately uploaded to the PHS production environment.

System Access
Industry standards and best practices state user access to any system should be appropriate based on the type of job duties of the user. During our audit of PHS, we found MSF did not have review procedures in place to identify inappropriate access and user accountability. As a result, we identified MSF employees with access to the system not required to perform their job duties. In addition, we identified active generic accounts which could be used for unauthorized activity in PHS where the specific user could not be identified. Finally, we identified an excessive number of users with access to PHS source code.

Recommendation #2
We recommend the department develop review procedures to identify and remove inappropriate access, including:
    A. Users whose access is not required of their job duties;
    B. Generic accounts; and,
    C. Users with unnecessary access to the production environment.

A. Recommendation Status: Implemented
MSF has implemented a documented review process of all system access. MSF produces a quarterly report of all business users, which is then reviewed by management for accuracy and

appropriateness. In addition, we reviewed the current PHS access list and found MSF has removed the inappropriate access identified in our audit.

B.   Recommendation Status: Implemented
As mentioned in the previous section, a review procedure has been implemented involving a quarterly management review of user access, including identifying existing generic accounts. We reviewed the current PHS access list and found the active generic accounts identified during our PHS audit have been removed.

C.   Recommendation Status: Implemented
MSF has limited access to the PHS production environment, including source code, to only system administrators. In addition, MSF has denied access to software engineers and programmers who have the knowledge to make changes to system source code. MSF has also implemented a review procedure requiring a bi-annual management review of this level of access to ensure appropriateness.

Additional Work
In December 2008, a financial-compliance audit of MSF (07-05) was presented to the Legislative Audit Committee. Within the audit report was a recommendation for MSF to implement review procedures to ensure access to computer systems is appropriate based on job duties. The recommendation was similar to our recommendation on system access. However, the recommendation was directed at a user access to another MSF system, ClaimCenter. During our follow-up work, we found the access review procedures implemented by MSF were not confined to the PHS, but were applied to all enterprise systems. As a result, we can also conclude MSF has implemented the recommendation made in the financial-compliance audit.

S:\Admin_Restricted\is\follow-up\08DP-01 MSF_Policy Holder System follow-up to orig_07DP-14.doc/bb